新軟週報
http://www.nusoft.com.tw
Internet Security Fighter
2011/4/1-2011/4/30 第126期

MLS / 郵件伺服器 系列報導

技術淺談與應用 - 不再擔憂郵件伺服器被列為黑名單

在多元化的網路時代，企業無不依賴電子郵件做為商業交流工具，帶給企業許多便利與商機。但也因電子郵件的便利，不少有心人士利用企業郵件伺服器安全性之漏洞，成為病毒郵件或垃圾郵件的轉送點，不僅將企業網路資源消耗殆盡，更嚴重導致郵件伺服器被列為黑名單，影響企業形象。

郵件伺服器被列為黑名單，常見的原因如下：

1.發送電子報或電子 DM：
未經收件人同意，直接發送大量廣告信，收件人易心生反感，視為垃圾信件， 並向 RBL 組織檢舉。

2.惡意程式 / 感染病蟲：
藉由病毒、木馬或惡意程式，在受感染的電腦內植入 Spam Relay 轉信引擎，透過受害者電腦作為跳板，然後自動啟用 SMTP 服務四處寄送病毒信，使電腦被列為廣告信主機，因此被 RBL 盯上。

3.Open Realy：
開放式的轉寄。管理人員沒將 SMTP 設定需要為認證，或者限定某些 IP 才能 Relay 而造成的人為疏失。使得有心人士利用 Open Relay 來傳送大量的訊息，以便偽裝真實的郵件來源進而隱藏自己的身分，讓無辜企業成為垃圾郵件的轉送點。

4.先前 IP 承租者問題：
先前有些 ISP 線路用戶的 IP 因發垃圾信被 ISP 停權，甚至列入即時黑名單，用戶退租後，若無人處理，IP 仍名列 RBL，等到下一個用戶使用時，會發現寄出的郵件都被阻擋。

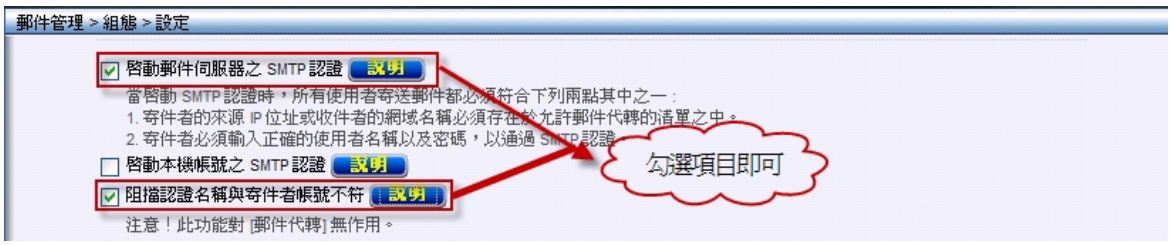
5.網路遭入侵盜用 / 不肖員工：
有些公司的郵件伺服器遭駭客入侵，或者員工利用公司本身網路資源，轉寄垃圾信，因此被 RBL 盯上。

為了避免上述之問題發生，新軟系統郵件伺服器 MLS / ML 系列產品，提供郵件寄送路由、郵件管制臨界值、SMTP 認證等幾種方式，解決企業郵件伺服器被當跳板，發送大量的垃圾郵件與病毒郵件，因而被列入為黑名單。

1.限制信件代轉對象

當郵件伺服器的代轉方式採用 Open Relay 時，非常容易被當作發送垃圾郵件的跳板，因而被反垃圾郵件組織列入黑名單；成為其他郵件伺服器的拒絕對象，影響正常的郵件聯繫。新軟郵件伺服器(MLS / ML)為了限制郵件代轉功能採用「郵件代轉設定」、「SMTP 認證」兩種方式；信件如需新軟郵件伺服器(MLS / ML)代為轉發，須滿足上述兩種條件之一。「郵件代轉設定」是“寄件者的來源 IP”或是“收件者之網域名稱”必須存在於允許郵件代轉的清單之中，新軟郵件伺服器(MLS / ML)才會代為轉發信件。「SMTP 認證」則是寄件者於寄信時必須通過 SMTP 認證，新軟郵件伺服器(MLS / ML)才會代為轉發信件。

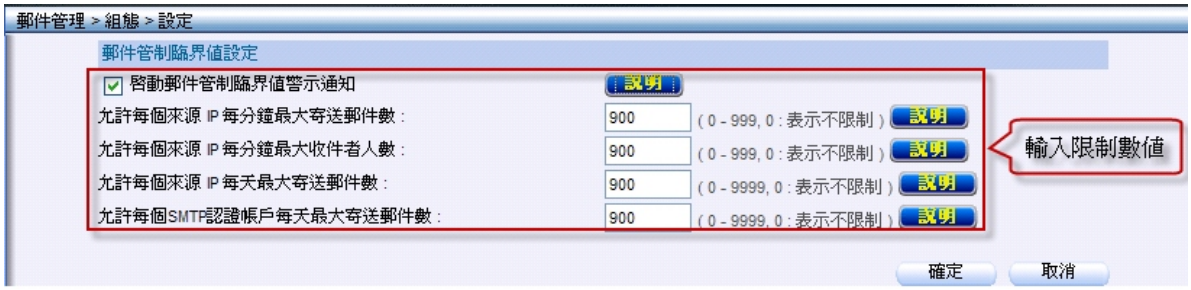
另外，需要注意的是當啟用 SMTP 認證功能時，若使用者之密碼過於簡單則容易會被垃圾郵件發送者所利用；反而成為垃圾郵件之跳板。因此，新軟系統郵件伺服器加入「阻擋認證名稱與寄件者帳號不符」功能，以阻擋上述情形之發生(一般垃圾郵件會偽造寄件者帳號，故認證名稱與寄件者帳號不同)。



圖一

2.郵件管制臨界值

如因使用者人為操作疏失（中毒、密碼過於簡單…）導致企業開始寄送垃圾郵件時，新軟郵件伺服器亦提供了「郵件管制臨界值」以避免事態擴大。本功能有「啟動郵件管制臨界值警示通知」、「允許每個來源 IP 每分鐘最大寄送郵件數」、「允許每個來源 IP 每分鐘最大收件者人數」、「允許每個來源 IP 每天最大寄送郵件數」、「允許每個核定帳戶每天最大寄送郵件數」幾種設定。可限定來源 IP 限制寄送郵件數、收件者人數…方式封鎖濫寄垃圾郵件的發生。並若有異常事件發生時，系統將會寄送通知信給管理人員；管理人員可立即察覺出問題所在，避免企業被列為黑名單。



圖二

3.「由內對外」垃圾郵件過濾機制

若上述防堵機制尚有漏網之魚時，新軟郵件伺服器亦內建了一般郵件伺服器所沒有的「由內對外垃圾郵件過濾」機制，可過濾從企業網路所發出的垃圾郵件。只要啟用「掃描本機帳號所寄出的信件」設定，即可將垃圾郵件以“直接刪除”、“轉送給收件者”、“儲存在隔離區”…方式處裡（由管理人員訂定處理方式，建議採用“儲存在隔離區”）。

圖三

4.郵件寄送路由

如果先前 IP 承租者發送垃圾信件，而被列入為黑名單，造成下一個 IP 用戶者寄出郵件都被阻擋。新軟郵件伺服器「MLS / ML 系列」提供「郵件寄送路由」功能。何謂郵件寄送路由？是將郵件伺服器所有寄送之郵件，先行寄送至 ISP 業者之 MTA 上，再統一透過此 MTA 轉送至目的郵件伺服器。當目的端郵件伺服器接收信件時，由於信件是由 ISP 之 MTA 所發送，所以信件之來源端位置將是「MTA 之 IP」而不是使用者所設置之「發信伺服器 IP」，藉由此方式解決先前 IP 用戶者不當，所造成的問題。

圖四

另外，新軟郵件伺服器提供「電子報」功能，以便訂戶可自行「新增訂閱」或「取消訂閱」，防止訂戶因電子報寄送，心生反感並視為垃圾郵件，向 RBL 舉發，因而被列為黑名單。

文 余光明 kongmeng@nusoft.com.tw

市場行銷報導 - 完整之 Backup 機制，保存企業重要的電子郵件

原本以為雲端很安全的 Gmail 用戶，在美國時間 2 月 27 號，全球約 0.08% 用戶的帳戶被清空，不論是信件、附件、分類的標籤或是聊天紀錄、部落格，全都不見。甚至有些用戶的 Gmail 還出現了新使用者才會有的「註冊成功歡迎信」；更有用戶在狀況發生不久後，還被暫時停權，無法登入。經此事件，才讓不少企業明白資料仍然需做備份，以免造成重要資料遺失，嚴重影響企業利益。

因此，新軟郵件伺服器 MLS / ML 系列產品中提供各種電子郵件相關機制(雙掃毒引擎、多重垃圾郵件過濾機制、Push Mail…)，當然也包含完整之 Backup 機制－「高可用性(HA)」、「電子郵件歸檔保存(Mail Archive)」、「遠端備份電子郵件(Remote Backup)」，來協助企業架構完整的電子郵件系統。

高可用性(High Availability)

何謂高可用性？就是雙主機備援機制，即時由備援設備取而代之。可避免發生不可預期的問題，導致相關工作頓時停擺時，有效減少郵件伺服器停止運作時間以維持電子郵件系統運作正常。一般郵件伺服器之硬體備援功能中，同步的資料包括「設定資料」、「使用者帳號與密碼」與「郵件」，其中以「郵件」資料最需要即時同步。因為在兩次資料同步的間隔期間，郵件伺服器發生問題而必須切換至備份主機時，尚未同步的郵件會從此消失了，而這些消失信件中有客戶訂單或重要之電子文件，後果不堪設想。

新軟系統高可用性功能與一般市用的高可用性不盡相同，因為新軟系統特別推出全新的硬體備援概念－「即時硬體備援(Real Time HA)」，就是隨時隨地同步雙方所有資料；正常運作的郵件伺服器所收到之信件，也讓備援主機同樣的時間內收到，完全沒有時間差的問題，在郵件伺服器發生問題時，電子郵件系統仍能正常運作。雖然雙主機備援需多買一台郵件伺服器，但高可用性功能有其必要性，它的作用就像是保險一樣為了以防萬一，不會因為郵件伺服器發生不可預期之問題，引發重要信件無法送達，進而造成信件遺失問題，損及企業商機。

電子郵件歸檔保存(Mail Archive)

企業要保存往來之電子郵件，除了以手動方式備份外，就只有建構「郵件備份伺服器」方能達到備份郵件之目的。雖然手動方式可以依使用者的需求，備份所需之信件，但也可能因人為疏忽而導致有些重要信件遺漏備份，且麻煩無比。「郵件備份伺服器」則簡單多了，會自動處理，完全沒有手動備份的麻煩。但是，企業需要額外增加電子郵件系統的建構成本，而且絕大部分的「郵件備份伺服器」並沒有篩選機制，因此正常郵件、垃圾郵件、病毒郵件…全部備份，真正有用的信件少之又少。

新軟系統為了協助企業節省備份郵件之建構成本，在其推出的郵件伺服器中加入「郵件歸檔」功能，可自動將企業往來信件歸檔存查，完全不需使用者手動備份或是額外添購「郵件備份伺服器」。除此之外，「郵件歸檔」功能亦可依照管理人員所設定之條件規則選擇所需要的信件備份，讓企業能更靈活備份其電子郵件。

遠端備份電子郵件(Remote Backup)

現在不少國家政府立法要求企業電子郵件需要保存五至七年，以便日後發生糾紛亦可以此為證，因此電子郵件要長久保存五至七年，容易造成郵件伺服器內建硬碟飽和問題，以及因天災/人禍或其他事故，導致原有郵件伺服器中斷服務，嚴重影響公司營運正常運轉。

為了上述之問題發生，新軟系統郵件伺服器提供了「遠端備份」功能，可將「郵件歸檔」的信件備份至 NAS、File Server、擁有網路芳鄰的電腦…方式。此種方式，除了備份空間大、全自動備份、使用磁碟陣列確保資料不損毀…外，在資料讀取查閱上也有著隨時隨地、方便、快速…的特性。另外，與其它郵件備份伺服器不同的是，新軟郵件伺服器的「遠端備份」加入「信箱災難復原機制」之功能，倘若內建硬碟損毀時，新軟郵件伺服器(MLS / ML 系列產品)在更換新的硬碟後，即會自動啟用「信箱災難復原機制」之功能，系統會依照設定值迅速將信件資料備份回所更換之新硬碟裡，包含：信件、通訊錄、WebDisk 裡的資料，通通會原封不動地回到每個使用者的信箱當中。

	Gmail	新軟郵件伺服器
建構方式	軟體安裝。	無。
備份機制	軟體備份。	遠端 NAS 備份機制。
適用儲存媒介	帳戶者本機電腦。	NAS、File Sever、擁有網路芳鄰的電腦。
自動 / 人工備份	使用「桌面端郵件軟體」、「Gmail Backup 軟體」備份信件，需人在旁操作軟體。	全自動備份，無須專人在旁操作。
備份信件瀏覽 / 找尋方式	在本機電腦資料夾中一封一封找尋所需之信件，花費時間長。	直接於管理介面瀏覽 / 搜尋信件，花費時間短。
瀏覽地點、時間	只能在本機電腦瀏覽信件。	在任何地點、時間，只需遠端連線至新軟郵件伺服器之控制介面，即可瀏覽信件。
信件保存時間	可永久保存，但出現人為疏失或者，導致資料將無法全部復原。	利用磁碟陣列不怕信件遺失。
復原機制	無。	只要啟動「信箱災難復原機制」及設定備份伺服器之位址，即可將整個信箱完整復原，成本相當低。

表1 - 比較備份機制的不同

文 余光明 kongmeng@nusoft.com.tw